REMARKS

The Examiner has rejected Claims 1-39 under 35 U.S.C. 103(a) as being unpatentable over Nikander et al. (U.S. Patent No. 6,253,321) in view of Fink (U.S. Patent No. 6,289,463). Applicant respectfully disagrees with such rejection.

With respect to independent Claims 1, 13, and 25, the Examiner has relied on the following excepts from Fink to make a prior art showing of applicant's claimed "masking the portion of outgoing network data to impersonate a different operating system in accordance with a security policy if the network is an untrusted network" (see this or similar, but not identical, language in each of the foregoing claims).

> "**Network link 120 typically provides data communication through one or more networks to other data devices.** For example, network link 120 may provide a connection through local network 122 to a host computer 124 or to data equipment operated by an Internet Service Provider (ISP) 126. ISP 126 in turn provides data communication services through the world wide packet data communication services through the world wide packet data communication network now commonly referred to as the "Internet" 128. Local network 122 and Internet 128 both use electrical, electromagnetic or optical signals which carry digital data streams. The signals through the various networks and the signals on network link 120 and through communication interface 118, which carry the digital data to and from computer system 100, are exemplary forms of carrier waves transporting the information." (Col. 5, lines 23-38-emphasis added)

> "A port grabbing process 275 is logically connected to each of the communications ports 260, 270. The port grabbing process 275 grabs all of the communication ports and opens each of the communication ports. The port grabbing process 275 then waits for a phone call coming in from the Unix calling system 200 and then passes the process to step 280. The port grabbing process 275 logically communicates with a processes password and skips welcome text routine 280 which in turn logically communicates with a call program routine 285. The port grabbing process 275 is logically connected to a Unix emulator process 290. **The communication between the Unix system 200 and the Windows NT system 250 is preferably conducted using asynchronous communication mode through the communication ports, although the communication can also be synchronous. ATM has been accepted universally as the transfer mode of choice for Broadband Integrated Services Digital Networks (BISDN).** ATM can handle any kind of information i.e. voice, data, image, text and video in an integrated manner. ATM provides a good bandwidth flexibility and can be used efficiently from desktop computers to local area and

> wide area networks. ATM is a connection-oriented packet switching technique in which all packets are of fixed length i.e. 53 bytes (5 bytes for header and 48 bytes for information). No processing like error control is done on the information field of ATM cells inside the network and it is carried transparently in the network. The communication can be either wired or wireless as is known. Advantageously, communications can be established between the calling Unix system 200 and the responding Windows NT system 250 without requiring any modification to the calling Unix system. As depicted in FIG. 2, the communications between Unix system 200 and Windows NT system 250 is conducted through ports 230, 270, respectively." (Col. 6, line 55-Col. 7, line 20- emphasis added)

Applicant respectfully asserts that the above excerpts from Fink simply disclose "provid[ing] data communication through one or more networks to other data devices" and "communication between the Unix system 200 and the Windows NT system 250 is preferably conducted using asynchronous communication mode through the communication ports, although the communication can also be synchronous" (see emphasized portion of excepts above).

Clearly, mere disclosure of communications between differing networks (e.g. Unix and Windows) and that such communication is preferably asynchronous, as in Fink, does not meet applicant's precise claim language. Specifically, the above excerpts, and the entire Fink reference, fail to teach "masking the portion of outgoing network data to impersonate a different operating system in accordance with a security policy if the network is an untrusted network" (emphasis added).

With respect to independent Claim 34, the Examiner has relied on the foregoing excerpts from Fink along with the following excerpt from Nikander to make a prior art showing of applicant's claimed "a data unit type field containing data representative of an identifier for a type of data unit, wherein information associated with the data unit is characteristic of an operating system; and an action field containing data representative of an action to be taken to mask the information associated with the data unit identified by the data unit type field."

> "Different sections of the block diagram in FIG. 3 have different performance requirements. The packet interceptor 303 potentially

> sees every packet in the network, including both IP packets and packets according to other protocols. It must be able to separate IP packets from the other packets and pass them on to the IPSEC engine 301 at the full supported packet rate. The IPSEC engine 301 normally sees every IP packet, and it must be able to process these packets also at the full supported packet rate. Both the packet interceptor 303 and the IPSEC engine 301 typically reside in an operating system kernel 308 of the computerized network device where the IPSEC implementation 300 takes place to minimize communication costs." (Col. 5, lines 41-53-emphasis added)

In combining independent Claim 34 with independent Claims 1, 13 and 25 in making the foregoing rejection, it seems the Examiner has failed to consider the entire weight of applicant's Claim 34. Specifically, Claim 34 includes claim language not incorporated into the foregoing independent Claims. Applicant respectfully asserts that nowhere in Fink nor Nikander is there any disclosure of "a data unit type field containing data representative of an identifier for a type of data unit...and an action field containing data representative of an action to be taken to mask the information associated with the data unit identified by the data unit type field" (emphasis added).

With respect to the foregoing excerpts relied on by the Examiner, and in addition to the arguments made above with respect to independent Claims 1, 13 and 25, Nikander simply teaches "see[ing] every packet in the network" and "separate[ing] IP packets from the other packets." This clearly fails to meet "a data unit type field containing data representative of an identifier for a type of data unit, wherein information associated with the data unit is characteristic of an operating system," as claimed by applicant. Thus, independent Claim 34 is simply not met by the Nikander and Fink references.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the

prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has substantially incorporated the subject matter of Claim 3 et al. into each of the independent claims.

With respect to the subject matter of dependent Claim 3 et al., presently incorporated in each of the independent claims, the Examiner has relied on the above cited excerpts from Nikander and Fink to meet applicant's claimed "replacing the portion of outgoing network data with data characteristic of the different operating system." Applicant respectfully disagrees with this assertion.

Applicant respectfully asserts that Fink's teaching of "provid[ing] data communication through one or more networks to other data devices" and "communication between the Unix system 200 and the Windows NT system 250 is preferably conducted using asynchronous communication mode through the communication ports, although the communication can also be synchronous" (see emphasized portion of excepts above) does not teach "replacing the portion of outgoing network data with data characteristic of the different operating system" (emphasis added). Fink completely fails to make any suggestion of replacing data in the context claimed by applicant.

The Examiner's rejections are also deficient with respect to the dependent claims. For example, with respect to dependent Claim 4 et al., the Examiner has relied on the following excerpt from Nikander to make a prior art showing of applicant's claimed "wherein the security policy identifies the portion of outgoing network data and specifies an action to take to mask the portion of outgoing network data."

> "The policy manager may also process a received non-regular packet by itself as an alternative to compiling new filter code and communicating it to the IPSEC engine. The designer of the policy manager may decide, what kind of non-regular packets are worth compiling new filter code and what kind of packets are most advantageously processed in the policy manager. Additionally the policy manager may process a received non-regular packet by itself and compile new filter code and communicate it to the IPSEC engine for the processing of further similar packets. The last alternative is especially applicable when the received packet is a key management packet." (Col. 8, lines 1-12-emphasis added)

Applicant respectfully asserts that Nikander simply discloses a policy manager that "may also process a received non-regular packet by itself as an alternative to compiling new filter code" (see emphasized excerpt above). Such teachings clearly do not meet applicant's claimed "security policy [that] identifies the portion of outgoing network data and specifies an action to take to mask the portion of outgoing network data." Allowing a policy manager to "process" or "compile new filter code" for a non-regular packet does not meet a "security policy" that "specifies an action to take to mask the portion of outgoing data," as claimed by applicant, since there is no mention of any type of masking, etc. in Nikander (emphasis added).

With respect to dependent Claim 5 et al., the Examiner has relied on the same excerpts from Fink and Nikander (cited above) as those with regard to each of the independent claims to make a prior art showing of applicant's claimed "wherein the security policy further specifies replacement data for the portion of outgoing network data, the replacement data characteristic of the different operating system."

Applicant again respectfully asserts that "provid[ing] data communication through one or more networks to other data devices" such as a "local network" and the "internet" (see Fink Col. 5, lines 23-38) in no way meets applicant's claimed "security policy" that "specifies replacement data...the replacement data characteristic of the different operating system." Simply nowhere in Fink or Nikander is there any mention of "replacement data," as claimed by applicant.

With respect to dependent Claim 10, the Examiner has relied on the following excerpt from Nikander to make a prior art showing of applicant's claimed "intercepting a portion of incoming network data; and sending a false response to the portion of incoming network data to impersonate the different operating system in accordance with the security policy if the network is an untrusted network."

> "A simple preferable embodiment of a method according to the invention is summarized as a flowchart in FIG. 5. Blocks 501 and 502 correspond to the operation of the packet interceptor 303 in FIG. 3, i.e. letting only IP packets reach the IPSEC engine. Blocks 503 to 507 describe operations that take place in the IPSEC engine. In block 503 the **IPSEC engine applies the filter code it has previously stored.** Applying the filter code in block 503 may include performing transformations on the packet, but this is not required by the invention. During the application of the filter code, the validity of the information stored in the IPSEC engine is also checked in block 503 for possible security association lifetime expirations or other invalidities. If the packet is a regular packet, the IPSEC engine knows whether it should drop the packet according to block 504 or accept it according to block 505; **an accepted packet is output according to block 506. If the application of the filter code involved performing a transformation or otherwise processing the packet, block 506 corresponds to outputting the processed packet.** If the answer in block 505 was no, the packet is non regular and it **must be transferred according to block 507 to the policy manager for examination and policy rule determination** according to block 508. The resulting new policy decisions are stored into the IPSEC engine at block 509 in the form of compiled filter code and the operation continues from block 503: the packet that caused the visit to blocks 508 and 509 has now become a regular one because the newly stored compiled filter code contains information about how the packet should be treated." (Col. 7, lines 39-67-emphasis added)

Applicant respectfully asserts that the above excerpt and the entire Nikander reference fail to disclose "sending a false response to the portion of incoming network data to impersonate the different operating system in accordance with the security policy if the network is an untrusted network" (emphasis added). The above excerpt merely teaches either "the accepted packet is output," "outputting the processed packed" or the packet is "transferred...to the policy manager for examination and policy rule determination" (see emphasized excerpt above) which completely fails to even suggest "sending a false response," as claimed by applicant.

Furthermore, with respect to dependent Claim 33, the Examiner has rejected applicant's claimed "wherein the computerized system is a firewall and the fingerprint masking process masks an operating system on a computer coupled the firewall" as being obvious. Specifically, the Examiner has stated that "[i]t would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Nikander et al so that the firewall would have missed the portion of outgoing network data to impersonate a different operating system in accordance with a security policy of the network is an untrusted network."

Applicant respectfully asserts that applicant's claimed "computerized system [being]... a firewall and the fingerprint masking process mask[ing] an operating system on a computer coupled the firewall" would not have been obvious. Specifically, applicant is claiming that the system in independent Claim 25, which includes a "masking process" not met by either the Nikander or Fink references, is a firewall. To further clarify the novelty of applicant's claim language, the only mention of a firewall in Nikander involves utilizing IP security protocol between firewalls, and not that the IP security protocol is a firewall, as claimed (see Col. 1, lines 17-21).

A notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 40-42 below, which are added for full consideration:

> "wherein the security policy contains data on a plurality of different operating systems for allowing the portion of outgoing network data to impersonate any one of the plurality of different operating systems" (see Claim 40);
>
> "wherein each of the different operating systems included in the plurality of different operating systems is assigned a specific untrusted network for

masking the portion of outgoing data according to the untrusted network" (see Claim 41); and

"wherein the false response is sent if the operating system would normally not respond to the incoming network data" (see Claim 42).

Again, a notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P350/01.022.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100